What is a blockchain?

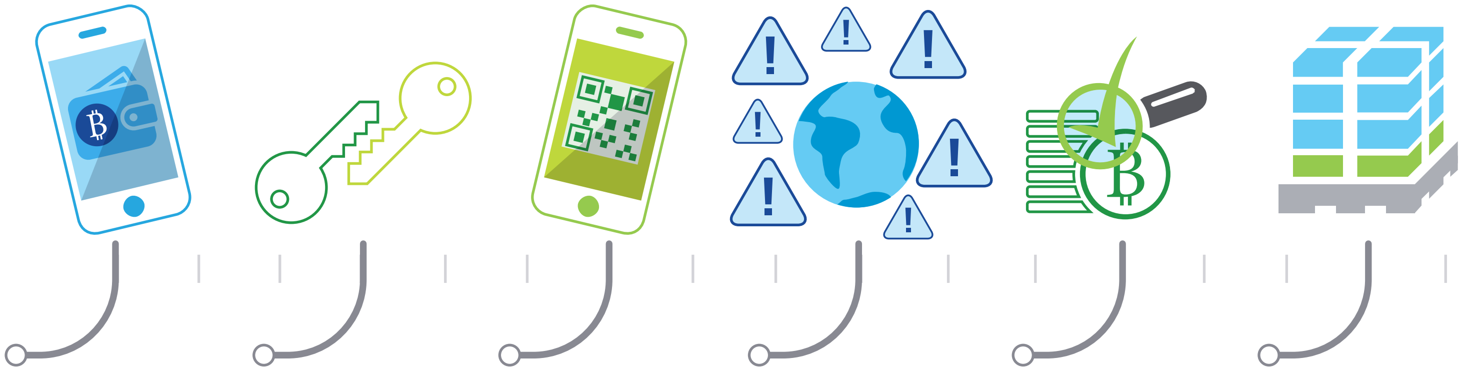
> "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination."[18]
>
> Satoshi Nakamoto

How does a blockchain work?

In his original Bitcoin white paper, Satoshi Nakamoto defined an electronic coin – the Bitcoin – as *"a chain of digital signatures"* known as the 'blockchain'.[19] The blockchain enables each coin owner to transfer an amount of currency directly to any other party connected to the same network without the need for a financial institution to mediate the exchange.

We can illustrate how a blockchain works by using Bitcoin as an example, as shown in Figure 1. Bitcoin, like other blockchains, uses cryptography to validate transactions, which is why digital currencies are often referred to as 'cryptocurrencies'. Bitcoin users gain access to their balance through a password known as a private key. Transactions are validated by a network of users called 'miners', who donate their computer power in exchange for the chance to gain additional bitcoins using a shared database and distributed processing.

Figure 1. How the Bitcoin blockchain works



Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

Graphic: Deloitte University Press. Source: American Banker[20]

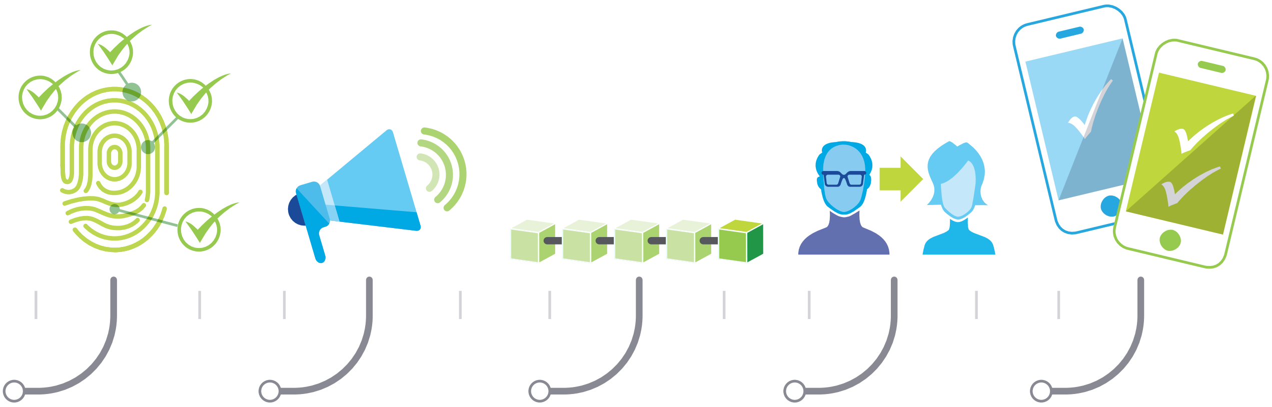
What is in a blockchain?

Despite its apparent complexity, a blockchain is just another type of database for recording transactions – one that is copied to all of the computers in a participating network.[21] A blockchain is thus sometimes referred to as a 'distributed ledger'. Data in a blockchain is stored in fixed structures called 'blocks'. The important parts of a block are:

- **its header**, which includes metadata, such as a unique block reference number, the time the block was created and a link back to the previous block

- **its content**, usually a validated list of digital assets and instruction statements, such as transactions made, their amounts and the addresses of the parties to those transactions.[22]

Given the latest block, it is possible to access all previous blocks linked together in the chain, so a blockchain database retains the complete history of all assets and instructions executed since the very first one – making its data verifiable and independently auditable. As the number of participants grows, it becomes harder for malicious actors to overcome the verification activities of the majority. Therefore the network becomes increasingly robust and secure. Indeed, blockchain solutions are being discussed as a potential means of protecting data from the UK's nuclear power stations, flood-defence mechanisms and other critical infrastructure.[23]



The new block is put in the network so that miners can verify if its transactions are legitimate. Verification is accomplished by completing complex cryptographic computations.

When a miner solves the cryptographic problem, the discovery is announced to the rest of the network.

The algorithm rewards the winning miner with 25 bitcoins, and the new block is added to the front of the blockchain. Each block joins the prior block so a chain is made – the blockchain.

Within ten minutes of Bob initiating the transaction, he and Alice each receive the first confirmation that the bitcoin was signed over to her.

All the transactions in the block are now fulfilled and Alice gets paid.

What are the differences between public and private blockchains?

Like many other types of database, blockchains can be public or private. The Bitcoin network is public (also called "permission-less") because anyone can read or write data from or to the ledger if they are running the appropriate Bitcoin software. Private blockchains, on the other hand, are networks where the participants are known *a priori* and have permission to update the ledger. Participants may come from the same organisation or from different organisations within an industry sector where the relationships between them are governed by informal arrangements, formal contracts or confidentiality agreements.

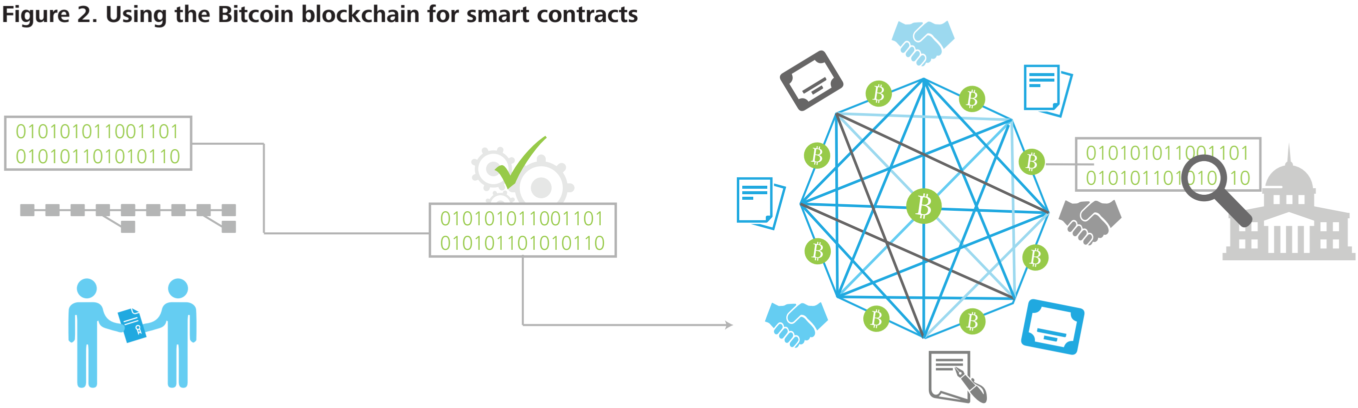
In the absence of trust, public blockchains typically require additional mechanisms to arbitrate disputes among participants and protect the integrity of the data. This involves added complexity because there is no central authority to arbitrate in a decentralised network. In the Bitcoin blockchain, for example, new transactions can only be added to the blockchain after a participant on the network solves a complex mathematical problem, known as a 'proof-of-work'. This process is called 'mining'. The effort miners have to expend on finding a solution to this mathematical problem acts as a sign that the transactions are valid, even though the miners may not know one another.

What alternatives are there to the Bitcoin blockchain?

Blockchains come in many different types. As well as the Bitcoin blockchain, a number of other independent blockchains have emerged in recent years. None has yet achieved the same scale as Bitcoin but they do offer other benefits, such as increased speed, larger data capacities, different consensus methods or more advanced functionality. Litecoin, for example, is a smaller competitor of Bitcoin but offers faster transaction times.[24] The Ripple Transaction Protocol is a variant of a distributed ledger providing instant, certified and low cost international payments targeted at banks and non-bank financial services companies.[25] Transactions on Ripple's distributed ledger are validated by consensus rather than using a proof-of-work approach like Bitcoin because a level of trust is assumed between the parties to a transaction.

Ethereum, on the other hand, is an open-source, crowd-funded project, much like the Bitcoin blockchain but which allows a network of peers to administer their own 'smart contracts' – short computer programmes carried on the blockchain that execute their instructions once certain criteria have been met.[26] It is these smart contracts that have the potential to transform business processes in many industry sectors. For example, Figure 2 illustrates how Bitcoin-based smart contracts could enhance transparency in investment banking.

Figure 2. Using the Bitcoin blockchain for smart contracts



1 An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is in the public ledger.

2 A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3 Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.

Graphic: Deloitte University Press, DUPress.com

In addition, technology companies like Microsoft are now providing 'Blockchain-as-a-Service' (BaaS) on their existing cloud platforms.[27] BaaS enables developers from any organisation to deploy private or semi-public blockchains using Bitcoin, Ripple, Ethereum and other protocols, and experiment with decentralised applications without incurring the capital costs associated with setting up their own networks.

What elements are common to all blockchains?

- **A blockchain is digitally distributed across a number of computers in almost real-time:** the blockchain is decentralised, and a copy of the entire record is available to all users and participants of a peer-to-peer network. This eliminates the need for central authorities, such as banks, as well as trusted intermediaries, such as brokerage firms.

- **A blockchain uses many participants in the network to reach consensus:** the participants use their computers to authenticate and verify each new block – for example, to ensure that the same transaction does not occur more than once. New blocks are only adopted by the network once a majority of its participants agree that they are valid.

- **A blockchain uses cryptography and digital signatures to prove identity:** transactions can be traced back to cryptographic identities, which are theoretically anonymous, but can be tied back to real-life identities with some reverse engineering.

- **A blockchain has mechanisms to make it hard (but not impossible) to change historical records:** even though all data can be read and new data can be written, data that exists earlier in a blockchain cannot in theory be altered except where the rules embedded within the protocol allow such changes – for instance, by requiring more than 50 per cent of the network to agree on a change.

- **A blockchain is time-stamped:** transactions on the blockchain are time-stamped, making it useful for tracking and verifying information.

- **A blockchain is programmable:** instructions embedded within blocks, such as "if" this "then" do that "else" do this, allow transactions or other actions to be carried out only if certain conditions are met, and can be accompanied by additional digital data.

> Blockchains come in many different types. As well as the Bitcoin blockchain, a number of other independent blockchains have emerged in recent years. None has yet achieved the same scale as Bitcoin but they do offer other benefits, such as increased speed, larger data capacities, different consensus methods or more advanced functionality.